

AD-A086 516

NAVAL POSTGRADUATE SCHOOL MONTEREY CA

F/G 9/4

SELECTION OF FOUR GOOD BINARY CODE WORDS FOR USE AS ADDRESSES A--ETC(U)

APR 80 6 A MYERS

NPS-62-80-010

NL

UNCLASSIFIED

1 cr 1
AL
ACROSS

END
DATE
FILMED
8 80
DTIC

100 II

25

ADA 086516

NAVAL POSTGRADUATE SCHOOL

Monterey, California



REC
COLLECTE
JUL 15 1980

A

DDC FILE COPY.

SELECTION OF FOUR GOOD BINARY CODE WORDS
FOR USE AS ADDRESSES AND A NOTE ON
ERROR CORRECTING CODES WITH REFERENCES

Glen A. Myers

April 1980

Approved for public release; distribution unlimited
Prepared for: Naval Undersea Warfare Engineering Station
Keyport, WA 98345

80 7 14 095

NAVAL POSTGRADUATE SCHOOL
Monterey, California

Rear Admiral J.J. Ekelund
Superintendent

Jack R. Borsting
Provost

The work reported herein was supported by the Naval Undersea Warfare Engineering Station, Keyport, WA 98345.

Reproduction of all or part of this report is authorized.

This report was prepared by:

Glen A. Myers
Glen A. Myers
Associate Professor of
Electrical Engineering

Reviewed by:

D.E. Kirk
D.E. KIRK, Chairman
Department of Electrical
Engineering

Released by:

William M. Tolles
W.M. TOLLES
Dean of Research

Accession for	
NTIS	✓
DDC	✓
Univ. of	✓
Johns Hopkins	✓
By	
Date	
Approved for release	
Authority	
Distr.	Special
A	

REPORT DOCUMENTATION PAGE		READ INSTRUCTIONS BEFORE COMPLETING FORM
1. REPORT NUMBER NPS-62-89-010	2. GOVT ACCESSION NO. AD-A086516	3. RECIPIENT'S CATALOG NUMBER
4. TITLE (and Subtitle) Selection of Four Good Binary Code Words for use as Addresses and a Note on Error Correcting Codes with References		5. TYPE OF REPORT & PERIOD COVERED
6. AUTHOR(s) Glen A. Myers		7. PERFORMING ORG. REPORT NUMBER
8. CONTRACT OR GRANT NUMBER(s)		9. PROGRAM ELEMENT, PROJECT, TASK AREA & WORK UNIT NUMBERS
10. PERFORMING ORGANIZATION NAME AND ADDRESS Naval Postgraduate School Monterey, California 93940		11. CONTROLLING OFFICE NAME AND ADDRESS Naval Undersea Warfare Engineering Station Keyport, Washington 98345
12. REPORT DATE Apr 1989		13. NUMBER OF PAGES 16
14. MONITORING AGENCY NAME & ADDRESS (if different from Controlling Office) 12/20		15. SECURITY CLASS. (of this report) UNCLASSIFIED
16. DISTRIBUTION STATEMENT (of this Report) Approved for public release; distribution unlimited		
17. DISTRIBUTION STATEMENT (of the abstract entered in Block 20, if different from Report)		
18. SUPPLEMENTARY NOTES		
19. KEY WORDS (Continue on reverse side if necessary and identify by block number) Selection of Four Good Binary Code Words		
20. ABSTRACT (Continue on reverse side if necessary and identify by block number) The criteria and procedure used to select good binary sequences is described. Both unipolar and bipolar logic are considered. Four good sequences, each having 20 bits, are identified for the choice of bipolar logic. The effects of errors in a sequence and random bits around a sequence are presented. A statement on error correcting codes and a list of chosen references is included.		

SELECTION OF FOUR GOOD BINARY CODE WORDS FOR USE AS ADDRESSES

Glen A. Myers

I. BACKGROUND

A matched filter (MF) is a linear system that maximizes at its output the ratio of peak signal power to average noise power where, in practice, the signal component of the input voltage is a pulse (time limited). In this sense, a MF is an optimum signal detector. The response of the MF to its matched signal $s(t)$ is the autocorrelation function (ACF) of the signal defined as

$$R_{ss}^p(t-t_0) = \int_{-\infty}^{\infty} s(\tau)s(\tau-t+t_0)d\tau \quad (1)$$

where t_0 is the amount of time the signal is delayed while passing through the filter. The ACF is even about its maximum value ($t=t_0$).

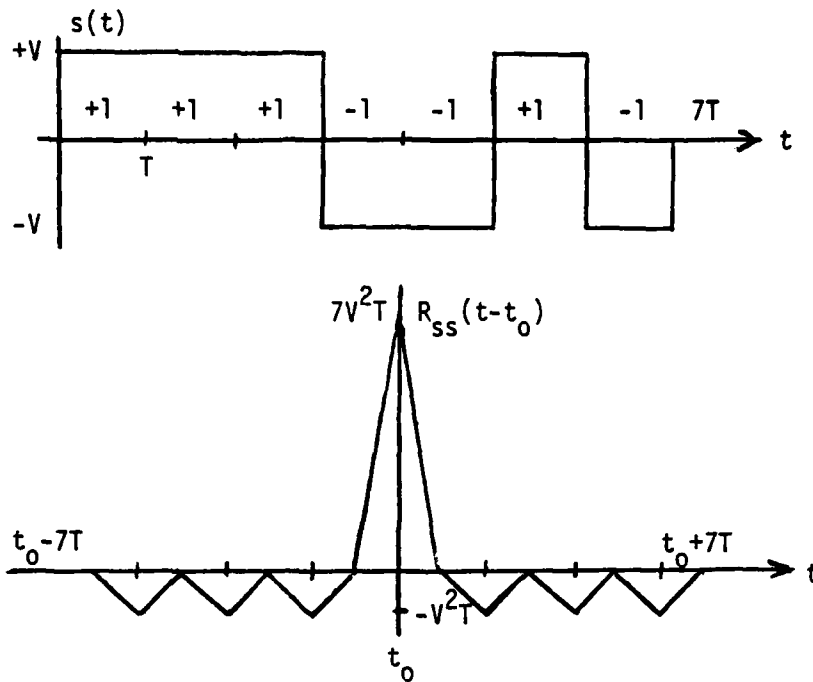
Of interest in this study is the ACF of binary sequences. In this case, $s(t)$ is digital (two-levels) with values defined here as $+V$ or $-V$ volts. It is convenient to normalize $s(t)$ to have values ± 1 volt (bipolar logic) or to have values $+1$ and 0 volts (unipolar logic). In all cases, the number N of symbols or bits in the sequence is the length of the sequence. For the binary case, the possible number of different sequences of length N is 2^N .

Since a digital $s(t)$ is piece wise constant, then the integrand of (1) is piece wise constant and so the ACF is piece wise linear. This means the ACF need be evaluated only at the end points of the linear segments (every T sec. or when $\tau = 0, \pm kT$ for $k = 1, 2, \dots, N-1$).

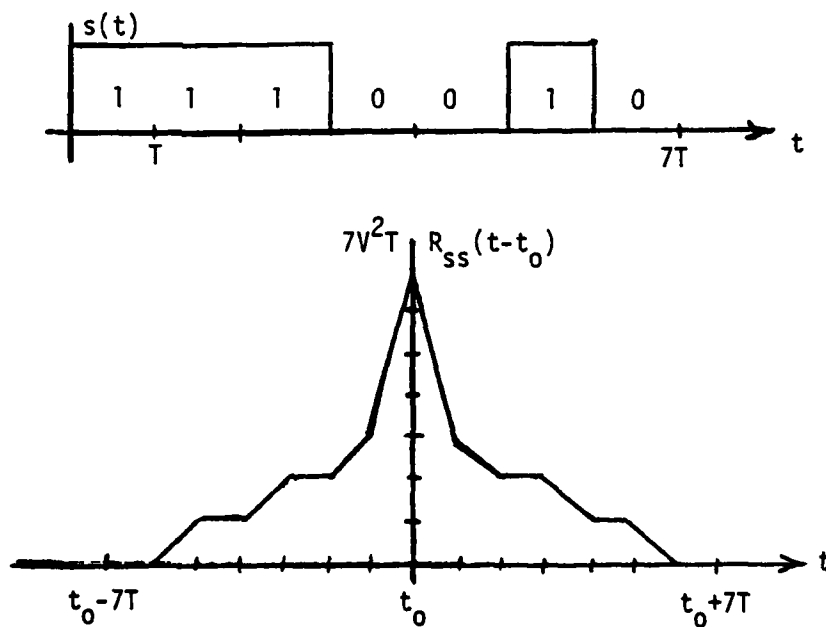
Fig. 1 shows a binary sequence of length 7 and its ACF. The values of the ACF at the linear segment end points are obtained by "clocking" the sequence past its stationary self and observing aligned pairs of bits.

For unipolar $s(t)$, then the value of the ACF is

$$(V^2T) (\text{number of positions where the bits are the same}) = V^2Tn_s \quad (2)$$



(a) Bipolar sequence and its ACF.



(b) Unipolar sequence and its ACF.

Fig. 1. A BINARY SEQUENCE OF 7 BITS AND ITS AUTOCORRELATION FUNCTION.

This result assumes the product operation of Equ. 1 is accomplished using an EXC NOR gate where $0 \cdot 0 = 1$. The maximum value of the ACF is, then, $V^2 T N$. In the rest of this report, we normalize the ACF to have a maximum value of N . Fig. 2 indicates the procedure used for the unipolar $s(t)$ and bipolar $s(t)$.

When $s(t)$ is bipolar, the value of the ACF is

$$V^2 T (n_s - n_d) = N - 2n_d \quad (3)$$

with n_d the number of positions where the bits are different. Again, the maximum value of the ACF is $V^2 T N$ which is normalized to N .

The cross-correlation function (CCF) of two binary sequences is obtained by "clocking" one sequence past the other and observing aligned pairs of bits. The value of the CCF is given either by Equ. 2 (unipolar logic) or Equ. 3 (bipolar logic). The CCF of two sequences of length 7 is given in Fig. 3.

It is particularly easy today to build a MF for any binary sequence of modest length (less than a few hundred symbols or bits). The circuitry needed to generate the ACF (MF synthesis) involves use of either a tapped delay line or a tapped read-only memory (ROM) as shown in Fig. 4. The delay line can be a shift register.

The output $\hat{R}_{ss}^D(t-t_0)$ of the circuits of Fig. 4 is a discrete version of the piece wise linear ACF $R_{ss}^D(t-t_0)$. The values of the ends of the linear segments are held for T seconds to form $\hat{R}_{ss}^D(t-t_0)$.

The objective of this study is to find a set of 4 binary sequences of length $N = 20$, each having "good" ACF and with each of the 6 possible CCF's having "small" maximum values.

A property of the ACF of binary sequences useful in this study is the following. Let A represent a binary sequence, \bar{A} the sequence with all symbols complemented, A_r the sequence A reversed (read backwards) and \bar{A}_r the complement of A_r . All of these sequences have the same ACF. Note that sometimes

+1	+1	+1	+1	+1	+1	-1	-1	+1	-1	stationary sequence
			-1	-1	+1	-1				clocked sequence
			↓	↓	↓	↓				
			different	different	same	same				

$$n_s = 2; n_d = 2$$

$$R_{ss}(t - t_0 + 3T) = V^2 T (n_d - n_s) = 0$$

(a) Value of ACF for bipolar sequence when $t = t_0 - 3T$.

1	1	1	1	1	1	1	0	0	0	1	0	stationary sequence
				0	0	1	0					clocked sequence
						↓	↓					
						same	same					

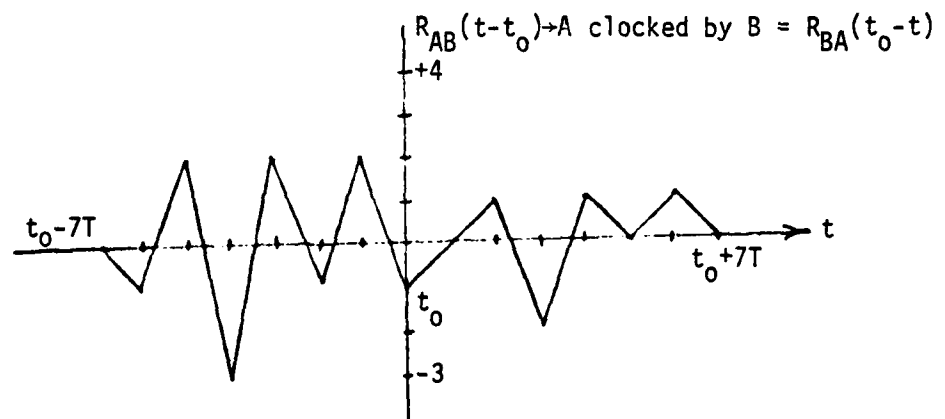
$$R_{ss}(t - t_0 + 3T) = V^2 T n_s = 2V^2 T$$

(b) Value of ACF for unipolar sequence when $t = t_0 - 3T$.

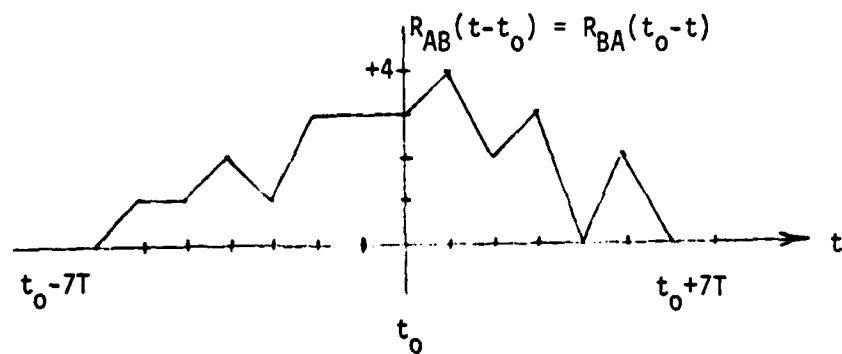
Fig. 2. ACF CALCULATION

SEQUENCE A \rightarrow +1 +1 +1 -1 -1 +1 -1

SEQUENCE B \rightarrow +1 -1 +1 -1 +1 -1 +1

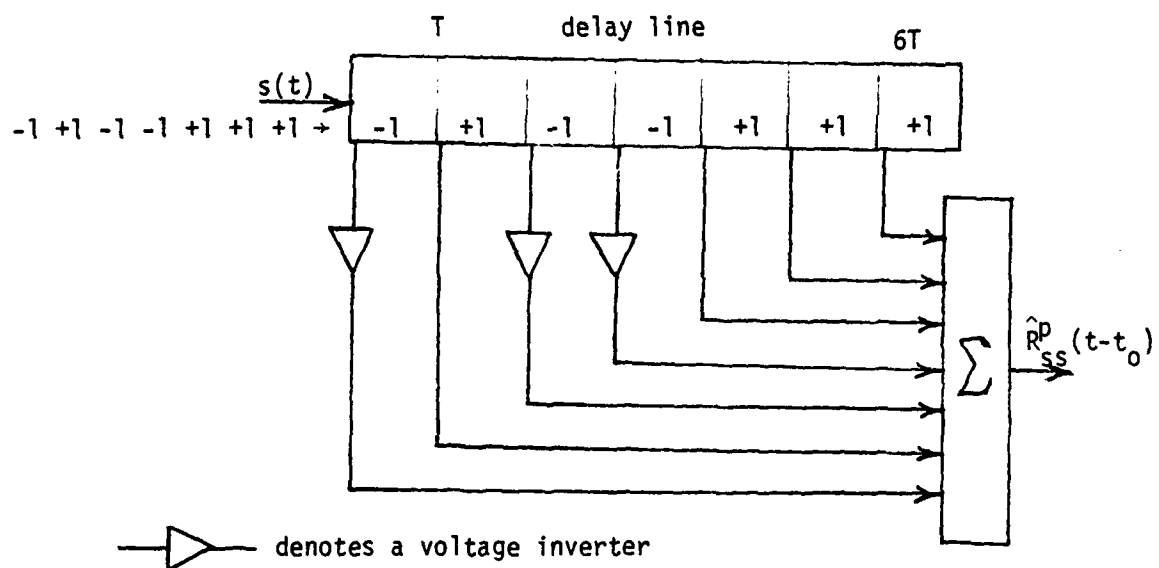


(a) Bipolar logic.

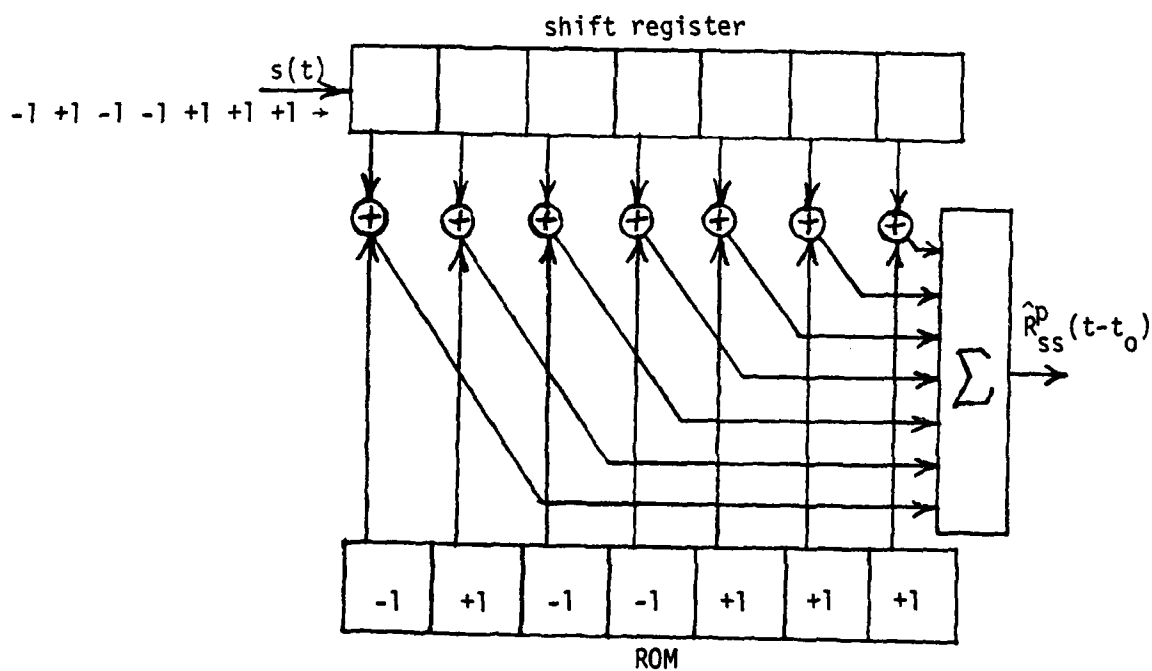


(b) Unipolar logic.

Fig. 3 CCF OF 2 SEQUENCES OF LENGTH 7 BITS.



(a) Tapped delay line



(b) Shift register

Fig. 4. CIRCUIT REALIZATIONS OF MF FOR BINARY SEQUENCES.

$A = A_r$ and sometimes $A = \bar{A}_r$. The number of sequences of length N having different ACF's is

$$2^{N-2} + \frac{2^{N/2}}{2}, N \text{ even} \quad (4)$$

$$2^{N-2} + \frac{2^{(N-1)/2}}{2}, N \text{ odd}$$

When $N = 20$, then the number of different ACF's is 262,656. [Ref. 1]

II. SELECTION OF SEQUENCES

When $N = 20$, there are $2^{20} = 1,048,576$ possible sequences. Consequently, a digital computer was used to identify candidate sequences. Both unipolar and bipolar sequences were considered.

Not all of the possible 2^{20} sequences were considered. It seemed reasonable to limit the search to sequences where the number of 1's in the sequence was $\approx \frac{N}{2} = 10$. Therefore, only codes having 8, 9, 10, 11, or 12 ones were considered. The computer printed those sequences and their ACF provided all secondary maxima of the ACF were less than a predetermined value.

1. Unipolar logic

No sequences having all secondary maxima of their ACF less than 8 exist. There are 1192 sequences having secondary maxima of their ACF less than or equal to 8. Of these 1192 sequences, 16 have 8 ones, 292 have 9 or 12 ones and 884 have 10 or 11 ones. Only 2 of these 1192 have an ACF secondary maxima of 8 at two instants while 170 have this value at three instants. The rest of the sequences have an ACF secondary maxima of 8 at 4 or more instants. A computer printout of these sequences and their ACF's is available.

These results make it difficult to select 4 sequences which are "better" than the rest. The two sequences having the "best" ACF and their ACF values (extrema) are listed in Fig. 5.

1	0	0	1	0	0	1	1	0	1	0	1	0	0	1	1	1	0	0	0
20	8	7	8	7	7	7	7	7	7	3	5	3	3	3	3	3	2	1	0
1	0	1	1	0	0	1	1	0	1	0	1	0	0	1	1	1	1	0	0
20	8	7	8	7	7	7	7	7	7	3	5	3	3	5	3	1	2	1	0

Fig. 5. TWO UNIPOLAR SEQUENCES AND THEIR ACF.

2. Bipolar logic

Three sequences having all secondary maxima of their ACF less than 2 exist. These 3 sequences are listed in Fig. 6 along with the values (extrema) of their ACF.

There are many (perhaps more than 500) sequences having all secondary maxima of their ACF less than or equal to 2. A computer printout of these sequences and their ACF's is available. Three of these sequences were selected somewhat arbitrarily. All do have the characteristic of small ripple in the sidelobe structure of their ACF. The sidelobe amplitudes vary from +2 to -3. The three selected sequences and their ACF are shown in Fig. 7.

Next, all possible CCF's of the 6 sequences of Figs. 6 and 7 were determined. A summary of the results is a tabulation of the largest and smallest values of the CCF as shown in Fig. 8.

In that table, the entries in the third column and first row result from aligning sequence S_1 with S_3 (20 bit comparison) and then sliding S_1 past S_3 . After incrementing 20 times, this gives $R_{S_1 S_3}^P(\tau)$ for $\tau > 0$. $R_{S_1 S_3}^P(\tau)$ for $\tau < 0$ can be obtained by aligning sequence S_3 with S_1 and sliding S_3 past S_1 . These results of interest are entered in column 1 and row 3. Use is then made of the relation

$$R_{S_1 S_3}^P(\tau) = R_{S_3 S_1}^P(-\tau). \quad (5)$$

After some inspection, it is concluded the four best sequences of these 6 of interest are S_1 , D_1 , D_2 and D_3 . The sidelobe levels of the four ACF's are all ≤ 2 . The sidelobe levels of the 6 possible CCF's are all ≤ 9 .

III. EFFECTS OF ERRORS AND RANDOM BITS

The correlation function calculations of Section II assumed no errors in the stored or received sequences. Further, it is assumed in Section II that no bits preceded nor followed the received sequence. In practice, neither of

$S_1 = 1 \ 0 \ 0 \ 1 \ 1 \ 1 \ 0 \ 0 \ 1 \ 0 \ 1 \ 1 \ 1 \ 0 \ 1 \ 0 \ 0 \ 0 \ 0 \ 0$
 ACF of $S_1 = 20 \ 1 \ 0 \ -1 \ 0 \ -3 \ 0 \ -1 \ 0 \ -1 \ 0 \ 1 \ 0 \ -3 \ 0 \ -1 \ 0 \ 1 \ 0 \ -1$

$S_2 = 1 \ 0 \ 0 \ 1 \ 0 \ 0 \ 1 \ 1 \ 0 \ 0 \ 0 \ 0 \ 1 \ 0 \ 1 \ 0 \ 1 \ 1 \ 1 \ 1$
 ACF of $S_2 = 20 \ -1 \ 0 \ 1 \ 0 \ -1 \ 0 \ 1 \ -4 \ -1 \ -2 \ 1 \ 0 \ -1 \ 0 \ -3 \ 0 \ -1 \ 0 \ 1$

$S_3 = 1 \ 0 \ 1 \ 1 \ 0 \ 1 \ 0 \ 0 \ 1 \ 1 \ 1 \ 1 \ 1 \ 0 \ 0 \ 0 \ 1 \ 0 \ 0 \ 0$
 ACF of $S_3 = 20 \ 1 \ 0 \ 1 \ -4 \ -1 \ 0 \ -1 \ 0 \ -1 \ -2 \ 1 \ 0 \ 1 \ 0 \ -3 \ 0 \ -1 \ 0 \ -1$

Fig. 6. THREE BIPOLAR SEQUENCES ($N = 20$) HAVING MAXIMUM SIDELobe LEVEL OF +1 AND THEIR ACF.

$D_1 = 1 \ 0 \ 0 \ 1 \ 1 \ 0 \ 0 \ 1 \ 0 \ 1 \ 0 \ 0 \ 0 \ 0 \ 1 \ 1 \ 1 \ 1 \ 0 \ 1$
 ACF of $D_1 = 20 \ -1 \ -2 \ -1 \ -2 \ 1 \ -2 \ 1 \ -2 \ -3 \ 2 \ -1 \ 2 \ -1 \ -2 \ -1 \ 2 \ 1 \ -2 \ 1$

$D_2 = 1 \ 0 \ 0 \ 1 \ 0 \ 1 \ 1 \ 0 \ 0 \ 0 \ 0 \ 0 \ 1 \ 1 \ 1 \ 0 \ 1 \ 1 \ 1 \ 0$
 ACF of $D_2 = 20 \ 1 \ -2 \ -1 \ -2 \ -3 \ 0 \ -1 \ 0 \ -1 \ -2 \ 1 \ 0 \ 1 \ 0 \ -1 \ -2 \ 1 \ 2 \ -1$

$D_3 = 1 \ 0 \ 0 \ 0 \ 1 \ 0 \ 0 \ 0 \ 1 \ 0 \ 1 \ 1 \ 0 \ 1 \ 0 \ 0 \ 1 \ 1 \ 1 \ 1$
 ACF of $D_3 = 20 \ -1 \ 0 \ 1 \ -2 \ -1 \ 2 \ -1 \ 2 \ 1 \ -2 \ -1 \ -2 \ 1 \ -2 \ -3 \ -2 \ -1 \ 0 \ 1$

Fig. 7. THREE BIPOLAR SEQUENCES ($N = 20$) HAVING MAXIMUM SIDELobe LEVEL OF +2 AND THEIR ACF.

Bipolar Sequence	s_1	s_2	s_3	D_1	D_2	D_3
s_1	+1, -3	+4, -9	+10, -5	+6, -6	+6, -5	+6, -5
s_2	+7, -7	+1, -4	+5, -13	+8, -6	+12, -5	+7, -7
s_3	+10, -7	+5, -4	+1, -4	+6, -8	+3, -2	12, -8
D_1	+7, -8	+11, -8	+5, -4	+2, -3	+5, -6	+8, -5
D_2	+6, -9	+12, -6	+3, -19	+7, -5	+2, -3	+9, -11
D_3	+6, -6	+6, -5	+8, -5	+5, -8	+4, -9	+2, -3

Fig. 8. TABULATION OF THE LARGEST AND SMALLEST VALUES OF THE CORRELATION FUNCTIONS OF THE 6 SEQUENCES OF FIGS. 6 AND 7. The entries along the diagonal of the table indicate the maximum and minimum values of the sidelobes of the auto-correlation function of the sequence.

these assumptions may be valid. We consider here the effects of errors in the sequence and then the effects of random bits which may lead and follow the sequence of interest.

1. Effect of errors in the sequence

A primary effect of errors in the received sequence is to nullify a correct response of the receiver. It is also possible for errors to create a false response. We now consider the effect of errors on the ACF and CCF (output of MF) with unipolar logic and with bipolar logic.

The receiver is assumed to respond if its MF output exceeds a fixed threshold. In the systems of Fig. 4, a level detector following the summer can be used to establish a threshold value = T volts where $T < N$. The value of T depends on the error probabilities assigned to the system operation.

a. Unipolar logic

In the ACF and CCF results, an error in the received sequence can either create a bit agreement where there was disagreement or it can create disagreement where there was agreement. Clearly, then, a single bit in error will either increase or decrease the correlation function by one unit at each shift position (see Equ. 2).

Further, two errors will cause the correlation function to increase two units, decrease two units, or remain the same with probabilities $1/4$, $1/4$ and $1/2$ respectively. Three errors can change the correlation function values by $+3$, $+1$, -1 , or -3 units with probabilities $1/8$, $3/8$, $3/8$, and $1/8$ respectively. Similar reasoning can be applied to four or more errors.

b. Bipolar logic

In the ACF and CCF results, an error in the received sequence can either create a bit agreement where there was disagreement, or it can create disagreement where there was agreement. Therefore, from Equ. 3, a single bit in error will either increase or decrease the correlation function by two units at each shift position.

Two errors will cause the correlation function to increase 4 units or decrease 4 units or remain the same with probabilities 1/4, 1/4, and 1/2 respectively assuming random equiprobable errors. Three errors can change the correlation function values by +6, +2, -2, or -6 units with probabilities 1/8, 3/8, 3/8, and 1/8 respectively.

Similar reasoning can be applied to 4 or more errors.

2. Effect of random bits around the address

In a typical application, the receiver does not know when the address arrives. Consequently, the receiver cannot be gated to accept only the address bits. Randomly occurring bits generated by system noise precede and follow the N bits of the address. The probability these random bits will create a false response is of interest.

a. Unipolar logic

To create a false response, then $n_s \geq T$. The probability $n_s = T < N$ in a sequence of N equiprobable bits is

$$\binom{N}{T} \left(\frac{1}{2}\right)^N \quad (6)$$

where () is the binomial coefficient.

The probability $n_s = (T+1) < N$ is

$$\binom{N}{T+1} \left(\frac{1}{2}\right)^N \quad (7)$$

Therefore, the probability $n_s \geq T < N$ in a sequence of N bits is

$$P_{FA}^U = \left(\frac{1}{2}\right)^N \sum_{i=0}^{N-T} \binom{N}{T+i} \quad (8)$$

For example, when $N = 20$, $T = 16$, we have

$$\left(\frac{1}{2}\right)^{20} \sum_{i=0}^4 \binom{20}{16+i} = \left(\frac{1}{2}\right)^{20} [4845 + 1140 + 190 + 20 + 1] = \frac{6196}{2^{20}} = 0.00591 \quad (9)$$

The conclusion is that a random sequence of 20 bits will exceed a threshold level of 16 about 6 times per 1000 bits. If $T = 17$, the frequency of occurrence becomes about 13 times per 10,000 bits.

b. Bipolar logic

To create a false response, then $n_s - n_d \geq T$. But, for random sequences, $n_d = N - n_s$ and so $2n_s - N \geq T$ or $n_s \geq \frac{T+N}{2}$.

The probability of a false response then becomes (for equiprobable random bits or sequences)

$$P_{FA}^B = \left(\frac{1}{2}\right)^N \sum_{i=0}^{\frac{N-T}{2}} \binom{N}{(T+N)/2 + i}, \quad T \text{ an even integer for } N \text{ even.} \quad (10)$$

When N is even, T is even because $n_s + n_d = 20 = \text{even}$ and so both n_s and n_d must be even or both must be odd. Hence $n_s - n_d$ is always even. Consequently, only even values of T are practical and need be considered. (Similarly, if N is odd, then MF output has odd values for continuous sequences.)

As an example, when $N=20, T=16$, we have

$$P_{FA}^B = \left(\frac{1}{2}\right)^{20} \left[\binom{20}{18} + \binom{20}{19} + \binom{20}{20} \right] = 0.000201 \quad (11)$$

c. Comments

Knowledge of the tolerable probability of false response due to random sequences and probability of error in the received sequence permits best choice of threshold and logic.

REFERENCE

1. Ioannis Anastasopoulos, "A Theoretical Study and Computer Search for Binary Sequences having Specific Autocorrelation Functions", MS Thesis, Naval Postgraduate School, Monterey, California, Dec 78, p 67.

ERROR CORRECTING CODES

Glen A. Myers

The purpose of this task is to investigate types of error control which can be used with the telemetry data. This brief note indicates what types of coding are possible and includes a list of applicable references.

Let m = number of message digits in a word

k = number of check digits in a word

$n = m + k$ = total number of digits in the word.

A fundamental result of interest is that for single error correction,

$$k \geq \log_2 (n + 1).$$

For example, when $n = 20$, then $k \geq 5$ and so $m \leq 15$.

A conclusion, then, is that error correction is not possible using a 20 bit word containing 16 message bits. At least 21 bits are required.

The four check digits can be used to detect errors. For example, one check digit could be assigned to each group of 4 bits in the 4 groups comprising the 16 bit word.

REFERENCES

1. Richard W. Hamming, Coding and Information Theory, Prentice-Hall, 1980.
2. K. Sam Shanmugam, Digital and Analog Communication Systems, Wiley, Chap. 9, 1979.
3. ITT Handbook, Reference Data for Radio Engineers, pp 38-16 to 38-28, 1968.
4. Shu Lin, An Introduction to Error Correcting Codes, Prentice-Hall, 1970.
5. Andrew J. Viterbi, "Convolutional Codes and Their Performance in Communication Systems", IEEE Transactions on Communications Technology, Vol. COM-19, no. 5, Oct 1971, pp 751-772.
6. Andrew J. Viterbi and Jim K. Amura, Principles of Digital Communication and Coding, McGraw-Hill, 1979.
7. Peterson and Weldon, Error Correcting Coding, The MIT Press, 2nd ed., 1972, pp 121, 238.

Distribution List

Defense Technical Information Center Cameron Station Alexandria, VA 22314	2
Dudley Knox Library Naval Postgraduate School Monterey, CA 93940	2
Dean W.M. Tolles, Code 012 Dean of Research Naval Postgraduate School Monterey, CA 93940	2
Prof. O.B. Wilson, Code 61W1 Department of Physics and Chemistry Naval Postgraduate School Monterey, CA 93940	1
Prof. Glen A. Myers, Code 62Mv Department of Electrical Engineering Naval Postgraduate School Monterey, CA 93940	2
Naval Undersea Warfare Engineering Station Keyport, WA 98345 ATTN: Mr. R.L. Marimon, Code 70	1
Naval Undersea Warfare Engineering Station Keyport, WA 98345 ATTN: CDR C. Gertner, Code 80	1
Naval Undersea Warfare Engineering Station Keyport, WA 98345 ATTN: Mr. R.L. Mash, Code 50	1
Naval Undersea Warfare Engineering Station Keyport, WA 98345 ATTN: Mr. Jay Chase, Code 7021	2
Naval Undersea Warfare Engineering Station Keyport, WA 98345 ATTN: Administration Department, Code 0115	5